Contribution ID: **139** Type: **Oral**

E2E Verifiable Shareholders Voting system on blockchain using Paillier cryptosystem with RSA key distribution

Contact Phone

+380991158293

Abstract

The author describes implementation components of secure verifiable public voting protocol between stakeholders in enterprise solutions with keeping the privacy of each vote and getting trusted result.
The text explores principals of homomorphic encryption, which is used for trusted arithmetic operations on cipher texts. The solution uses Shamir key sharing protocol to generate key pair of system in distributed way. Additionally author explains the role of blockchain in this system as secure, immutable and transparent kind of storage.In contrast with other solutions for e-voting this study solves the problem of stakeholders by generation appropriate number of keys for each voter.
The author concludes that such kind of e-voting implementation gives a lot of advantages comparing with other solutions : keeping privacy , refusing from trusted key diller, temper-proof storage.

Type of Book of Abstracts

Electronic

Primary author: Mr MUNIN, Vladyslav

Presenter: Mr MUNIN, Vladyslav

Session Classification: Computer Technologies

Track Classification: Computer Technologies